CLAIMS

1. A security system for controlling access to one or more application functions located on a server or accessible via server, each application function having an associated security level, wherein one or more clients communicate with said server by means of requests for accessing one of said application functions using a network, wherein access to said application functions is controlled by security requirements, comprising:

an authentication component functionally separated from said clients and said application functions for processing said client request independently of said client type, containing more than one authentication mechanisms and selecting and executing an authentication mechanism from said more than one authentication mechanisms based on the information contained in the client request resulting in a security state;

a security component containing a security policy describing security requirements (security level) for accessing application functions, comparing said security state associated with said client with the security level of the application function and allowing access to the application function if the security state fulfills the security level.

2. A system according to claim 1, wherein said clients are PVC-devices.

3. A system according to claim 1, wherein said authentication component and said security component are integrated in one component stored on a server.

4. A system according to claim 1, whereby said authentication component consists of security plug-ins whereby each authentication mechanism is laid down in a separate security plug-in.

5. A system according to claim 4, whereby the authentication mechansim may be UserID/Password, Challenge/Response or digital signature.

6. A system according to 2 further comprising:

a component (ADL) for converting PVC-device specific requests into canonical requests before said request is used by said authentication component.

7. A method for controlling access to one or more application functions stored on a server or accessible via server, each application function having an associated security level, wherein one or more clients communicate with said server by means of requests for accessing one of said application functions using a network, whereby access to said application functions is controlled by a security requirements, comprising the steps of:

routing all incoming requests created by said clients to an authentication component which is functionally independent from said clients and said application functions, said authentication component comprising the steps of:

authentication of said client by determining an authentication mechanism provided by said authentication component by means of authentication information contained in said request and applying said authentication mechanism;

storing a result of said authentication and said authentication information or parts of it contained in said request as a security state;

using security requirements for said one of said application functions to be accessed;

comparing said stored security state with said security requirements for accessing the requested application function ; and

invoking said requested application function if said security state fulfills said security requirements.

8. A method according to claim 7 wherein said incoming requests are canonical requests.

9. A method according to claim 8 wherein said canonical requests are created by a Device Adaptation Layer which converts client specific requests into canonical requests.

10. A method according to claim 7 comprising the further steps of:

creating a session identifier when establishing a communication between a client and a server and using said session identifier in all requests and responses between said client and said server.

11. A method according to claim 10 whereby said session identifier and said security state are placed in a cookie, whereby said cookie is inserted into each request and response between said client and said server.

12. A method according to claim 7 wherein said clients are PVC-devices.

13. A computer program comprising computer program code portions for performing respective steps of the method according to claim 7 to 12 when the program is executed in a computer.

14. A computer program product stored on a computer-readable media containing software code for performing of the method according to one of the claim 7 to 12 if the program product is executed on the computer.

15. A client-server system, wherein one or more clients, having client types, communicate with a server by means of requests for accessing application functions located on or accessible via said server, wherein access to said

application functions is controlled by a security system located on said server, wherein said security system comprises:

an authentication component, functionally separated from said one or more clients and said application functions for processing client requests independently of client type, containing one or more authentication mechanisms and selecting and executing an authentication mechanism from said authentication mechanisms based on the information contained in the client request, resulting in a security state;

a security component containing a security policy describing security requirements (security level) for accessing application functions, comparing said security state associated to a client with the security level of the application function and allowing access to the specified application function if the security state fulfills the security level.